privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Aide-mémoire sur les risques et les mesures spécifiques à la technologie du Cloud

1 Introduction

Dans le cadre du traitement des données, les organes publics utilisent les prestations de tiers de manière très variée. Pour ce qui est de la sous-traitance du traitement des données à des tiers, la législation sur la protection des données (et sur l'information) comporte régulièrement des normes qui, pour l'essentiel, précisent que l'organe public :

- peut sous-traiter le traitement des données si des obligations légales de garder le secret (comme le secret de fonction selon l'art. 320 CP, les obligations particulières de garder le secret ou le secret professionnel) ou des actes conventionnels ne s'y opposent pas dans le contexte concret,
- doit s'assurer que les tiers traitent les données (personnelles) comme l'organe public le ferait lui-même,
- doit veiller en particulier à ce que les tiers soient en mesure de garantir la sécurité de l'information,
- reste globalement responsable également lors d'une sous-traitance du traitement des données.

La manière d'assumer cette responsabilité, dans le cas de **sous-traitants en matière de traitement de données**, a été précisée par diverses autorités de protection des données dans des guides ou des check-lists[1].

Aujourd'hui, les traitements des données se fondent toujours plus souvent sur l'utilisation de la **technologie du Cloud**[2] et des offres semblables qui comportent un risque élevé[3] pour la protection des données.

Privatim, la Conférence des Préposé(e)s suisses à la protection des données, a pour objectif d'indiquer, dans le présent aide-mémoire, les risques découlant de l'utilisation de la

1 Voir les liens dans l'annexe.

2 Voir à ce sujet la définition de « Cloud Computing » du National Institute of Standards and Technology (NIST) sous <https://csrc.nist.gov/publications/detail/sp/800-145/final>.

3 On pense ici aux offres de prestations qui ne contiennent pas tous les critères d'une certaine définition du Cloud Computing, mais qui présentent les mêmes risques.

privatim
c/o préposé à la protection des données du canton de Berne
Poststrasse 25, 3072 Ostermundigen
Tél. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

technologie du Cloud et des prestations similaires. Ceux-ci s'ajoutent ou s'accentuent **par rapport aux risques causés par la sous-traitance traditionnelle du traitement des données** à des tiers. Enfin, il s'agira de montrer comment les organes publics peuvent concrètement assumer leur responsabilité. Dans un souci de simplification, on parle ci-après uniquement de services du Cloud, mais les explications s'appliquent à toutes les sous-traitances du traitement des données qui comportent un risque élevé.

L'aide-mémoire se concentre sur les risques liés à la protection des données. Les organes publics doivent eux-mêmes gérer les autres risques concernant leurs activités, notamment ceux liés au respect des dispositions contractuelles ou qui ont trait à la souveraineté des données.

2 Domaines comportant un risque élevé lors du traitement des données dans le Cloud

Lorsque l'on se sert de la technologie du Cloud de sous-traitants, des risques existent ou s'accentuent dans divers domaines. L'organe public responsable doit exclure ou réduire ces risques à un niveau acceptable par des mesures adéquates ; si cela n'est pas possible, il convient alors de renoncer au service du Cloud. Lors de l'analyse des risques dans le traitement concret des données, il convient de tenir compte des risques spécifiques au Cloud et de prendre les mesures nécessaires.

Cinq risques particuliers doivent être traités de manière prioritaire :

- conception du contrat (chiffre 2.1 ci-après),
- lieux des traitements des données, y compris les accès des autorités étrangères (chiffre 2.2),
- confidentialité, protection des secrets, cryptage et gestion des clés (chiffre 2.3),
- données concernant les utilisatrices et utilisateurs des services du Cloud (chiffre 2.4),
- contrats de sous-traitance (chiffre 2.5).

Le risque lié à la technologie du Cloud est principalement déterminé par ces cinq risques.

Il faut y ajouter d'autres risques qui sont au moins accentués par l'utilisation d'une infrastructure du Cloud : devoirs d'annonce (chiffre 2.6), droit et possibilité de contrôle (chiffre 2.7), mesures de sécurité de l'information (chiffre 2.8) et obligations en cas de résiliation du contrat (chiffre 2.9). Enfin, il faut aussi tenir compte du fait que les dépendances envers le fournisseur de prestations (disponibilité, dépenses dues à la migration en cas de changement) continuent à augmenter.

2.1 Conception du contrat

L'organe public doit conclure un contrat écrit avec le fournisseur de services du Cloud. Alternativement, il conclut un contrat-cadre ou accepte des conditions générales (CG) qui respectent les exigences indiquées dans le présent aide-mémoire et qui ne peuvent pas être modifiées de manière unilatérale.

Il convient de tenir compte de trois aspects en particulier :

- L'organe public doit élaborer les obligations contractuelles de comportement et de diligence du fournisseur de sorte qu'elles remplissent toutes les conditions que lui-même doit respecter selon la législation sur la protection des données qui s'applique à lui. En particulier, le fournisseur ne peut traiter *que* les données et seulement *de la manière* dont l'organe le ferait lui-même[4].

  De plus, le fournisseur doit participer à l'exécution des droits des personnes concernées découlant de la législation sur la protection des données (prétentions de l'effacement des données et de la correction des données).

- L'organe public doit pouvoir contrôler que les obligations contractuelles sont respectées (voir le chiffre 2.7 ci-après).

- La défense des obligations contractuelles devant des tribunaux faciles d'accès pour l'organe public doit être possible selon un régime juridique connu de lui.

  En principe, une relation contractuelle doit être soumise au droit suisse et il faut convenir d'un for en Suisse pour les décisions portant sur des conflits découlant du contrat.

  Dans des cas justifiés, il est possible de convenir que le droit d'un autre Etat et un for étranger s'appliquent s'il n'y a aucun risque supplémentaire pour les droits fondamentaux des personnes concernées, notamment, lorsque :

  - les données peuvent être protégées de manière efficace, par le biais du cryptage, contre l'accès de tiers (et même du fournisseur du service Cloud [chiffre 2.3]) ou,

  - sous condition qu'il ne s'agit pas de données particulières[5], si la législation sur la protection des données[6] dispose d'un niveau de protection équivalent et que des sanctions efficaces et dissuasives menacent le fournisseur en cas de violation (p. ex. RGPD de l'UE).

2.2 Lieux des traitements des données, y compris les accès des autorités étrangères

Le fournisseur de services du Cloud doit déclarer dans quels Etats il exploite son infrastructure Cloud pour le traitement des données personnelles (y c. celles selon le chiffre 2.4) afin que l'organe public puisse évaluer la licéité des transferts de données à l'étranger

---

4 Principe de proportionnalité (minimisation des données, durée de conservation, etc.) et finalité (le fournisseur ne peut pas traiter des données personnelles à d'autres fins que celles qui sont autorisées à l'organe public lui-même) ; ces deux aspects s'appliquent aussi aux données concernant les utilisatrices et utilisateurs des services du Cloud selon le chiffre 2.4.

5 Le terme « données particulières » est utilisé dans le présent document comme terme générique pour toutes les données personnelles avec un besoin de protection élevé, c'est-à-dire les données personnelles sensibles, les profils de la personnalité et les données personnelles sous l'obligation légale de garder le secret.

6 Les parties ne peuvent pas choisir la législation sur la protection des données ; celle-ci découle du champ d'application personnel, à raison de la matière et à raison du lieu de la législation sur la protection des données elle-même.

et, dans le cadre de l'évaluation des risques, prendre en considération les risques liés aux lieux où se trouvent les serveurs.

- Les traitements de données qui s'effectuent en Suisse doivent être préférés (sécurité de l'infrastructure, p. ex. en relation avec les objectifs de protection comme la disponibilité, l'intégrité des données, l'imputabilité ou la traçabilité, ainsi que l'accessibilité aux contrôles, voir le chiffre 2.7).

- Les traitements de données dans des lieux étrangers[7] ne sont licites que dans les Etats qui ont un niveau de protection des données équivalent[8] ou dans lesquels une protection des données adéquate peut être atteinte contractuellement, notamment par des clauses contractuelles standard reconnues. Ce n'est pas le cas lorsque, dans l'Etat en question, des accès par les autorités sont possibles qui ne satisfont pas aux garanties constitutionnelles des droits fondamentaux (principe de légalité, principe de proportionnalité, droits des personnes concernées, accès à des tribunaux indépendants). Dans ce cas, il faut prendre des mesures supplémentaires (en particulier un cryptage efficace) afin que le transfert de données personnelles à l'étranger soit licite.

Attention : les fournisseurs de services[9] soumis au CLOUD Act[10] doivent accorder aux autorités nord-américaines un droit d'accès aux données enregistrées. Celui-ci doit être accordé même si la sauvegarde n'intervient pas aux Etats-Unis, mais, par exemple, dans un Etat de l'Union européenne ou en Suisse. L'accès d'une autorité en vertu du CLOUD Act ou un décret juridique similaire d'un autre Etat serait considéré comme une communication illicite à des tiers, parce qu'elle aurait lieu sans base légale reconnue par la Suisse. Il faut tenir compte, dans l'analyse, du risque d'une telle violation du droit, et réduire ce risque autant que possible par des mesures contractuelles (surtout l'obligation du fournisseur de Cloud de saisir toutes les voies de recours pour empêcher la divulgation des données et informer immédiatement l'organe public des demandes de communication par des autorités dans la mesure où le fournisseur de Cloud y est autorisé[11]).

2.3 Confidentialité, protection des secrets, cryptage et gestion des clés

a. Toutes les données personnelles

Les données personnelles traitées par le fournisseur du Cloud (y c. celles selon le chiffre 2.4) doivent être protégées contre les accès non autorisés de tiers. Indépendamment du fait qu'il s'agisse de données personnelles « simples » ou particulières, elles doivent être

---

7 Sous traitement des données à l'étranger, il faut aussi comprendre l'accès d'un lieu à l'étranger à des données sauvegardées en Suisse (p. ex. pour des services d'assistance), puisque, dans ce contexte, les données sont transmises à l'étranger, du moins temporairement.

8 Voir la liste des pays du PFPDT sous <https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html>.

9 Pour savoir qui est soumis au CLOUD Act, voir le livre blanc du département de la Justice des Etats-Unis d'avril 2019, en particulier la page 8 : <https://www.justice.gov/opa/press-release/file/1153446/download>.

10 Clarifying Lawful Overseas Use of Data Act (CLOUD Act), H.R. 4943, <https://www.congress.gov/bill/115th-congress/house-bill/4943>.

11 Dans la mesure où des autorités peuvent accéder sans en informer l'organe public responsable, on ne peut pas évaluer la probabilité d'occurrence (parce qu'elle est invérifiable) de sorte que l'attention porte sur l'étendue des dommages où la qualité des données est déterminante (données personnelles particulières).

cryptées, du moins lors de leur transmission (« data in transit »), selon l'état actuel de la technologie.

La confidentialité doit être préservée par des mesures appropriées lorsque le fournisseur du Cloud traite les données. Tant que cela est réalisé par le cryptage, il convient de noter que les données sauvegardées par cryptage (« data at rest ») ne restent pas cryptées sur une base régulière durant la suite de leur traitement (« data in process »)[12].

b. Données personnelles sensibles

En cas de données personnelles sensibles, il faut tenir compte, en plus, du fait que plusieurs risques ou tous les risques mentionnés ici en lien avec la confidentialité pour les services du Cloud existent. Il faut alors poser des exigences plus élevées pour préserver la confidentialité des données et les prendre en compte dans la gestion des risques :

- Les données doivent être cryptées et le cryptage doit être réalisé par l'organe public. Les clés ne doivent être disponibles que pour l'organe public. Elles doivent être protégées de la perte et de la soustraction, ainsi que de l'utilisation et de la prise de connaissance abusives.

- Un cryptage peut être envisagé chez le fournisseur de services du Cloud seulement si cela ne fait pas encourir des risques inacceptables aux droits fondamentaux des personnes concernées (ce que l'organe public doit indiquer de manière pertinente). Dans ce cas, il faut tenir compte du niveau auquel le cryptage a lieu (application, banque de données ou disque dur). Le fournisseur de services du Cloud peut conserver les clés s'il s'engage par contrat à les utiliser uniquement avec le consentement exprès de l'organe public. Il faut tenir un procès-verbal des accès. De plus, le fournisseur du service du Cloud doit protéger les clés de la perte et de la soustraction, ainsi que de l'utilisation et de la prise de connaissance abusives. Il doit aussi garantir que les données ne soient pas compromises lors du processus de cryptage.

c. Données personnelles sous l'obligation légale de garder le secret

Les données personnelles qui sont soumises à une obligation légale de garder le secret ne peuvent être accessibles au fournisseur du Cloud (et, le cas échéant, à son sous-traitant) seulement dans la mesure où la disposition concernant la sauvegarde du secret en question permet de recourir à des auxiliaires. Cette disposition doit aussi déterminer quelles sont les personnes auxiliaires qui entrent en ligne de compte et quelles exigences doivent être remplies pour que la protection des secrets soit assurée. La violation des dispositions concernant la sauvegarde du secret sans motif justificatif reconnu doit être considérée comme une entrave juridique de la sous-traitance et pas seulement comme un risque.

2.4 Données concernant les utilisatrices et utilisateurs des services du Cloud

En règle générale, les fournisseurs (du Cloud) ne traitent pas seulement les données personnelles transmises par l'organe public dans les services du Cloud (en particulier les données de contenu), mais aussi celles générées par eux-mêmes ou leurs services par

12 Cela s'applique notamment lors de l'utilisation des offres de la plate-forme en tant que service (PaaS) et du logiciel en tant que service (SaaS).

l'intermédiaire des utilisatrices et utilisateurs (p. ex. des données secondaires, de télémétrie ou de journalisation). Ces données personnelles supplémentaires doivent être traitées avec la même diligence que celles que traite l'organe public pour accomplir ses tâches. Elles doivent être soumises aux mêmes dispositions contractuelles et il faut garantir de la même manière la licéité de leur traitement et de leur protection. Il faut régler, notamment, le respect des droits des personnes concernées et la suppression après un délai de conservation approprié ou requis par la loi et les soutenir par des mesures adéquates.

Ces données personnelles supplémentaires doivent être enregistrées et exploitées exclusivement à des fins qui seraient aussi autorisées à l'organe public ; elles doivent être communiquées à l'organe de manière transparente. En général, il s'agit de buts qui n'ont pas un caractère personnel. Entrent en ligne de compte la planification et le rapport des capacités techniques, le maintien de la sécurité de l'information et des services, la maintenance technique de l'infrastructure ou la saisie des frais dépendant de l'utilisation, par exemple. Des traitements pour d'autres finalités sont licites uniquement si les données sont recueillies de manière anonyme, préalablement anonymisées ou efficacement pseudonymisées.

Selon le contexte, il convient de noter que les données personnelles supplémentaires peuvent devenir des données personnelles sensibles (p. ex. lorsque des données de connexion indiquent que la personne concernée séjourne dans un hôpital psychiatrique ou dans un établissement pénitentiaire).

2.5 Contrats de sous-traitance (subcontracting)

L'organe public demeure aussi responsable des traitements de données que le fournisseur du Cloud transmet, pour sa part, à des tiers (y compris à la société-mère et à la société-fille). C'est pourquoi, avant la conclusion du contrat entre l'organe public et le fournisseur, ce dernier doit annoncer ses contrats de sous-traitance individuellement de façon à ce que l'organe public ait la possibilité d'évaluer la licéité des transferts de données vers l'étranger et les risques en lien avec tous les prestataires de services du Cloud impliqués. Le contrat doit indiquer les mesures par lesquelles le fournisseur du Cloud instruit et contrôle ses sous-traitants (y c. les relations avec les [chaînes de] sous-sous-traitants).

Les sous-traitants issus de pays qui n'ont pas un niveau de protection des données adéquat devraient être exclus ; si une protection des données insuffisante pour cause d'accès éventuel des autorités ne peut pas être compensée contractuellement, il est illicite d'y recourir.

Pendant la durée du contrat, toute modification dans les contrats de sous-traitance doit être annoncée au préalable à l'organe public avec la possibilité de résiliation.

2.6 Devoirs d'annonce

Le fournisseur de services du Cloud doit annoncer à l'organe public toute modification dans la manière de traiter les données (en particulier les lieux de traitement des données, les sous-traitances) et tout événement lié à la sécurité conformément à la législation sur la protection des données applicable, ainsi que les mesures prises pour les maîtriser afin qu'il puisse prendre à temps des dispositions en relation avec le service du Cloud.

2.7 Droit et possibilité de contrôle

L'organe public doit conserver le droit d'effectuer des contrôles : le fournisseur doit s'engager à procéder à des contrôles réguliers de ses services du Cloud selon des standards internationaux reconnus et les exigences en matière de protection. Les rapports de contrôle doivent être remis, sur demande, à lui-même et à l'autorité de la protection des données compétente. Si nécessaire (notamment si les contrôles du fournisseur ne couvrent pas tous les points et qu'ils se limitent, p. ex., aux aspects sécuritaires), des contrôles de l'organe lui-même ou de son autorité de la protection des données ou de tiers mandatés par cette dernière doivent être possibles.

2.8 Mesures de sécurité de l'information

L'organe public doit s'assurer que ses exigences de protection sont garanties pour toutes les données personnelles traitées. Pour ce faire, il doit obliger le fournisseur de services du Cloud à déclarer les objectifs de sécurité et les mesures de sécurité de l'information avec lesquelles il entend les atteindre.

Le fournisseur de services du Cloud doit exploiter ses services du Cloud selon les besoins de protection et les standards internationaux reconnus et le prouver, le cas échéant, avec les certificats adéquats.

2.9 Obligations en cas de résiliation du contrat

Le processus à respecter en cas de résiliation du contrat de service doit être convenu au moment de sa conclusion (en particulier la restitution des données et leur suppression).

3 Conclusions

Dans la mesure où ils respectent les règles qui leur sont imposées pour une sous-traitance du traitement des données (voir les documents référencés dans l'annexe), les organes publics peuvent aussi se servir de la technologie du Cloud fournie par un tiers. A cet effet, il est nécessaire de tenir compte des risques spécifiques liés aux services du Cloud dans le cadre d'une analyse de risque globale. Cette analyse doit être faite de manière différenciée pour tous les traitements de données. Elle doit démontrer les risques et les mesures concrètes avec lesquelles on entend exclure la réalisation du risque, respectivement avec lesquelles on diminue le risque dans une mesure acceptable. Une telle analyse des risques doit établir si, pour un traitement donné, l'utilisation des services du Cloud est globalement, partiellement ou pas du tout licite.

Sur le fond, la sous-traitance du traitement des données ne doit pas porter préjudice aux droits fondamentaux des personnes concernées. Pour que les risques supplémentaires découlant de l'utilisation des services du Cloud paraissent néanmoins acceptables, les organes publics doivent démontrer, dans chaque cas concret, par quels avantages incontournables des services du Cloud ils peuvent compenser les nouveaux risques par rapport à une solution équivalente *on premise* et aussi en regard des produits d'autres fournisseurs comportant un faible risque.

Les organes publics qui utilisent les services du Cloud pour accomplir leurs tâches restent globalement responsables du traitement des données. L'organe public (resp. la direction

au plus haut niveau[13]) doit confirmer par écrit qu'il a compris les risques et qu'il est prêt à assumer les risques résiduels[14]. La prise en compte des risques résiduels peut avoir une conséquence sur la comptabilité, ce qui devrait être vérifié par le contrôle des finances. Il est conseillé à l'Exécutif de prendre régulièrement connaissance de ces risques (résiduels), car c'est lui qui répond, face au Parlement et à la population, du respect des droits fondamentaux des citoyennes et des citoyens et des agissements financiers de l'administration. Vu que les services du Cloud évoluent constamment et que, dans le cadre du renouvellement régulier des contrats d'utilisation de durée déterminée, les conditions de protection des données non négociables ne peuvent pas être modifiées, il ne faut pas, dès le début, perdre de vue les scénarios de sortie auxquels l'organe public peut recourir au cas où des changements provoqueraient des risques inacceptables.

L'organe public doit procéder à une analyse d'impact sur le plan de la protection des données. Il convient de soumettre une analyse des risques et un plan des mesures aux autorités de la protection des données compétentes (contrôle préalable et consultation préalable) conformément à la législation sur la protection des données. Ces autorités conseillent les organes publics également sur les questions juridiques, organisationnelles et techniques.

---

13 S'agissant de la mise en place de services du Cloud dans l'ensemble d'une administration, il faut considérer le Gouvernement comme étant la direction au plus haut niveau de la collectivité publique en question.

14 Contrairement au droit privé sur la protection des données, où les responsables peuvent assumer pour l'essentiel chaque risque portant sur l'atteinte à la personnalité, les organes publics ne peuvent pas évaluer à leur libre appréciation si un risque semble être acceptable eu égard aux droits fondamentaux des personnes concernées et, de ce fait, qu'il peut être assumé. Ce sont surtout les dispositions constitutionnelles, et en particulier le principe de proportionnalité, qui sont déterminantes.

Annexe : guides sur la sous-traitance du traitement des données par des préposé(e)s cantonaux à la protection des données

Canton de Bâle-Campagne	Aide-mémoire Outsourcing
Canton de Bâle-Ville	Site Internet « Handreichungen » Guide sur la sous-traitance du traitement des données
Canton de Genève	Fichier « Cloud computing et protection des données personnelles au sein des institutions publiques genevoises »
Canton de St-Gall	Aide-mémoires et outils de travail
Canton de Vaud	Check-list pour un contrat de sous-traitance de solution informatique
Canton de Zurich	Site Internet Auslagerung Guide Bearbeiten im Auftrag Guide Auslagerung CLOUD-Act Guide Verschlüsselung der Datenablage im Rahmen der Auslagerung Aide-mémoire Cloud Computing